

**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ
ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)**

Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

УТВЕРЖДАЮ

**Первый проректор – проректор по
учебной работе**

Г.М. Машков

2021 г.

Регистрационный № 11.05.19/532



РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ПРАКТИКИ

(наименование вида практики)

программа подготовки специалистов среднего звена

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
(код и наименование специальности)

квалификация
техник по защите информации

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования и учебным планом программы подготовки специалистов среднего звена среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утверждённым ректором ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» 27 мая 2021 г., протокол № 5.

Составитель:
Преподаватель


(подпись)

Н.В. Кривоносова

СОГЛАСОВАНО
Главный специалист НТБ УИОР


(подпись)

Р.Х. Ахтреева

ОБСУЖДЕНО
на заседании предметной (цикловой) комиссии № 5 (информатики и программирования в компьютерных системах)
07 апреля 2021 г., протокол № 8

Председатель предметной (цикловой) комиссии:


(подпись)

Н.В. Кривоносова

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций
21 апреля 2021 г., протокол № 6

Зам. директора по УР колледжа СПб ГУТ


(подпись)

О.В. Колбанёва

СОГЛАСОВАНО

Директор колледжа СПб ГУТ


(подпись)

Т.Н. Сиротская

СОГЛАСОВАНО

Директор департамента ОКОД


(подпись)

С.И. Ивасишин

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	5
3. СТРУКТУРА И СОДЕРАНИЕ УЧЕБНОЙ ПРАКТИКИ	7
4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	10
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ	21

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

1.1. Область применения программы

Рабочая программа учебной практики – является частью основной образовательной программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (квалификация – техник по защите информации) в части освоения основных видов деятельности:

- Эксплуатация информационно-коммуникационных систем и сетей;
- Защита информации в информационно-коммуникационных системах и сетях с использованием программных, программно-аппаратных, в том числе криптографических средств защиты;
- Защита информации в информационно-коммуникационных системах и сетях с использованием технических средств защиты.

Область профессиональной деятельности выпускников: Область профессиональной деятельности выпускников: 06 Связь, информационные и коммуникационные технологии. 12 обеспечение безопасности¹.

1.2. Цели и задачи - требования к результатам освоения учебной практики

Практика имеет целью комплексное освоение обучающимися всех основных видов деятельности по специальности среднего профессионального образования, формирование общих и профессиональных компетенций, а также приобретение необходимых умений и опыта практической работы по специальности.

Учебная практика по специальности направлена на формирование у обучающихся умений, приобретение первоначального практического опыта и реализуется в рамках профессиональных модулей по основным видам деятельности для последующего освоения ими общих и профессиональных компетенций по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (квалификация – техник по защите информации).

В результате освоения программы учебной практики обучающийся должен уметь и иметь первоначальный практический опыт по основным видам деятельности

Основной вид деятельности	Умения и первоначальный практический опыт
Эксплуатация информационно-телекоммуникационных систем и сетей	монтаж, настройка, проверка функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей (далее –ИТКС);
	текущий контроль функционирования оборудования ИТКС; диагностика технического состояния приёмо-передающих устройств и линейных сооружений связи и источников питания;
	проведения технического обслуживания, диагностики технического состояния, поиска неисправностей и ремонта оборудования ИТКС;
	текущий контроль функционирования оборудования ИТКС; мониторинг технического состояния и работоспособности приёмо-передающих устройств и линейных сооружений связи и источников питания ИТКС;
Защита информации в информационно-телекоммуникационных системах и сетях	установка, настройка, испытаний и конфигурирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС;
	поддержание бесперебойной работы программных и программно-аппаратных (в том числе криптографических) средств защиты информации в ИТКС

¹Приказ Министерства труда и социальной защиты Российской Федерации от 29 сентября 2014 г. № 667н «О реестре профессиональных стандартов (перечне видов профессиональной деятельности)» (зарегистрирован Министерством юстиции Российской Федерации 19 ноября 2014 г., регистрационный № 34779).

Основной вид деятельности	Умения и первоначальный практический опыт
с использованием программно-аппаратных, в том числе криптографических средств защиты	защита информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты в соответствии с предъявляемыми требованиями;
	установка, монтаж, настройка и испытание технических средств защиты информации от утечки по техническим каналам
	установка, монтаж, настройка и испытание технических средств защиты информации от утечки по техническим каналам;
	проведение технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
	защита информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
	проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации.

1.3. Количество часов на освоение рабочей программы учебной практики

Всего – 396 часов (11 нед.), в том числе:

В рамках освоения ПМ.01 – 108 часов

В рамках освоения ПМ.02 - 108 часов

В рамках освоения ПМ.03 – 108 часов

В рамках освоения ПМ.04 – 72 часа

2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Результатом освоения программы учебной практики является сформированность у обучающихся практических профессиональных умений, приобретение первоначального практического опыта, необходимых для последующего освоения ими и общих (ОК) и профессиональных (ПК) компетенций по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (квалификация – техник по защите информации).

Код	Наименование результата обучения по специальности
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности

Код	Наименование результата обучения по специальности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере
ПК1.1.	Производить монтаж, настройку и поверку функционирования и конфигурирования оборудования информационно – телекоммуникационных систем и сетей.
ПК 1.2.	Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно – телекоммуникационных систем и сетей.
ПК 1.3.	Проводить техническое обслуживание оборудования информационно – телекоммуникационных систем и сетей
ПК 1.4.	Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей
ПК 2.1.	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей
ПК 2.2.	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях
ПК 2.3.	Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.
ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно – телекоммуникационных системах и сетях.
ПК 3.2.	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях
ПК 3.3.	Осуществлять защиту информации от утечки по техническим каналам в информационно – телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
ПК 3.4.	Проводить отдельные работы по физической защите линий связи информационно – телекоммуникационных систем и сетей

3 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

3.1. Структура учебной практики

Коды профессиональных компетенций	Наименования профессионального модуля и его разделов	Учебная практика (часов)
1	2	3
	ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей	108
	МДК.01.01 Приемно-передающие устройства, линейные сооружения связи и источники электропитания	108
	МДК.01.02 Телекоммуникационные системы и сети	
	МДК.01.03 Электрорадиоизмерения и метрология	
	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	108
	МДК.02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	54
	МДК.02.02 Криптографическая защита информации	54
	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	108
	МДК.03.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	72
	МДК.03.02. Физическая защита линий связи информационно-телекоммуникационных систем и сетей	36
	ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (для специальностей СПО)	72
Всего часов		396

3.2. Содержание учебной практики

Код и наименование профессиональных модулей, МДК и тем учебной практики	Содержание учебных занятий		Объём часов на УП	Уровень освоения

Код и наименование профессиональных модулей, МДК и тем учебной практики	Содержание учебных занятий		Объем часов на УП	Уровень освоения

4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Лаборатория «Защиты информации от утечки по техническим каналам».

Лаборатория должна быть оснащена средствами защиты информации от утечки по акустическому (виброакустическому) каналу; средствами защиты информации от утечки по каналам, формируемым за счет побочных электромагнитных излучений и наводок; средствами контроля эффективности защиты информации от утечки по акустическому (виброакустическому) каналу и каналам побочных электромагнитных излучений и наводок;

шумогенераторы;
комплексный поисковый прибор;
прожигатели телефонных линий;
устройство обнаружения скрытых видеокамер;
виброакустические генераторы;
подавители диктофонов;
подавители устройств сотовой связи;
устройство защиты аналоговых сигналов;
устройство защиты цифровых сигналов;

стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения, охранно-пожарной сигнализации и охраны объектов;

комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

4.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации имеет электронные издания и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

Нормативные документы:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

11. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.
12. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
13. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
15. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
16. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
17. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
18. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
19. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
20. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
21. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недеklarированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
23. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
24. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
25. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
27. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
28. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
29. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

30. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
31. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
32. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
33. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
34. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
35. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
38. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
40. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
41. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
42. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
43. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
44. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
45. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
46. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
47. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

4.2.1. Электронные издания:

1. Баранова, Е.К. Основы информационной безопасности: учебник для студ. учреждений СПО / Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2019.
2. Берлин, А. Н. Высокоскоростные сети связи: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016.
3. Берлин, А. Н. Оконечные устройства и линии абонентского участка информационной сети: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016.
4. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: учебное пособие для вузов/Г.А.Бузов. - Москва: Горячая линия-Телеком, 2018.

5. Зайцев, А. П. Технические средства и методы защиты информации: учебник для вузов / А.П.Зайцев, Р.В.Мещеряков, А.А.Шелупанов. – 7-е изд., испр. – Москва: Горячая Линия–Телеком, 2018.
6. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019.
7. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учреждений СПО /В.Я.Ищейнов, М.В.Мецагунян. - Москва: Форум: ИНФРА-М, 2018.
8. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. - Москва: Юрайт, 2020.
9. Криптографическая защита информации: учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — Москва: РИОР: ИНФРА-М, 2020.
10. Портнов, Э. Л. Оптические кабели связи, их монтаж и измерение: учебное пособие для вузов / Э.Л. Портнов. - Москва: Горячая линия-Телеком, 2012.
11. Программно-аппаратные средства обеспечения информационной безопасности / А.В.Душкин, О.М.Барсуков, Е.В.Кравцов, К.В.Славнов. – Москва: Горячая Линия–Телеком, 2016.
12. Родина, О.В. Волоконно-оптические линии связи: практическое руководство/О.В.Родина. - Москва: Горячая линия-Телеком, 2016.
13. Смычек, М.А. Технологические сети и системы связи: учебное пособие / М.А. Смычек. - 2-е изд. - Москва; Вологда: Инфра-Инженерия, 2019.
14. Соколов, С.А. Волоконно-оптические линии связи и их защита от внешних влияний: учебное пособие / С.А. Соколов. – М.: Инфра-Инженерия, 2019.
15. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие/П.Б.Хорев. - 2-е изд., испр. и доп. - Москва: Форум: ИНФРА-М, 2020.
16. Цуканов, В.Н. Волоконно-оптическая техника: практическое руководство/ В.Н. Цуканов, М.Я. Яковлев. – Москва: Инфра-Инженерия, 2019.
17. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. - Москва: ФОРУМ: ИНФРА-М, 2020.

Электронные ресурсы:

1. RusCable.Ru. Энергетика. Электротехника. Связь: отраслевое электронное СМИ. – URL: <http://www.ruscable.ru/>.
2. Волхонский, В.В. Устройства охранной сигнализации/В.В.Волхонский; НИУ ИТМО. – Текст: электронный. - Санкт-Петербург: Университет ИТМО, 2015. – URL: https://books.ifmo.ru/book/1633/ustroystva_ohrannoy_signalizacii.htm
3. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова. - Екатеринбург: Изд-во Урал. ун-та, 2019. – URL: http://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf
4. Каторин, Ю.Ф. Защита информации техническими средствами: учебное пособие / Ю.Ф.Каторин, Разумовский А.В., Спивак А.И. под редакцией Ю.Ф. Каторина. – С.-Петербург: НИУ ИТМО, 2012. – URL: <https://books.ifmo.ru/file/pdf/975.pdf>
5. Марусина, М.Я. Метрологическое обеспечение средств измерений: учебное пособие М.Я.Марусина, В.Л.Ткалич, Р.Я.Лабковская.. – СПб: Университет ИТМО, 2019. – URL: <https://books.ifmo.ru/file/pdf/2422.pdf>
6. Пленкин, А.П. Построение, измерения и тестирование проводных линий связи телекоммуникационной сети. Часть 1: Методическая разработка /А.П.Пленкин, Ю.В. Зачиняев. –URL: <http://open-edu.rsu.ru/files/Методичка%20№4.pdf>
7. Пленкин, А.П. Построение, измерения и тестирование проводных линий связи телекоммуникационной сети. Оптическое волокно. Часть 2: Методическая разработка/А.П.Пленкин. - Таганрог, 2016. – URL: <http://open-edu.rsu.ru/files/Методичка%20№5.pdf>
8. Руководство по применению адресно-аналоговых систем пожарной сигнализации/ С.М. Щипицын, А. Н. Членов, И. В. Павлов, А. Е. Атаманов. –Москва: Систем Сенсор Фаир

Детекторс, 2012// СИГМА: группа компаний: официальный сайт. – URL: http://www.sigma-is.ru/files/education/Rukovodstvo_AASPS_2012.pdf.

9. Рыжова, В.А. Проектирование и исследование комплексных систем безопасности/В.А.Рыжова; НИУ ИТМО. –С.-Петербург: НИУ ИТМО, 2013. – URL: <https://books.ifmo.ru/file/pdf/1018.pdf>
10. Теория информационной безопасности и методология защиты информации /Ю.А.Гатчин, В.В.Сухостат, А.С.Куракин, Ю.В.Донецкая. –2-е изд., испр. и доп. – С.-Петербург: Университет ИТМО, 2018. – URL: <https://books.ifmo.ru/file/pdf/2372.pdf>
11. Техническая эксплуатация линейных сооружений: учебное пособие/ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики»; колледж связи. – Самара, 2017. – URL: http://ks.psuti.ru/downloads/students/distance_learning/3МТС-74,75/МДК.В.01.05%20Техническая%20эксплуатация%20линейных%20сооружений/МДК.01.05%20Учебное%20пособие.pdf
12. Энциклопедия инструментов: иллюстрированный справочник по инструментам и приборам. – URL: <http://www.tools.ru/tools.htm>.

4.2.3. Дополнительные источники:

1. Андреев, В.А. Направляющие системы электросвязи: учебник для вузов. В 2 т. Т.1. Теория передачи и влияния/ В.А.Андреев, Э.Л.Портнов, Л.Н.Кочановский. - Москва: Горячая линия-Телеком, 2011.
2. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. - Москва: Юрайт, 2020.
3. Башлы, П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва: РИОР, 2013.
4. Берлин, А. Н. Абонентские сети доступа и технологии высокоскоростных сетей: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016.
5. Берлин, А. Н. Телекоммуникационные сети и устройства: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016.
6. Ворона, В. А. Инженерно-техническая и пожарная защита объектов / В.А. Ворона, В.А. Тихонов. - Москва: Горячая Линия–Телеком, 2012.
7. Ворона, В.А. Системы контроля и управления доступом/В.А.Ворона, В.А.Тихонов. - Москва: Горячая линия-Телеком, 2013.
8. Ворона, В.А. Технические системы охранной и пожарной сигнализации /В.А.Ворона, В.А.Тихонов. - Москва: Горячая линия-Телеком, 2012.
9. Ворона, В.А. Технические средства наблюдения в охране объектов / В.А. Ворона, В.А. Тихонов. - Москва: Горячая линия-Телеком, 2011.
10. Голиков, А.М. Тестирование и диагностика в инфокоммуникационных системах и сетях [Электронный ресурс]: учебное пособие / А.М. Голиков. – М.: ТУСУР, 2016.
11. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие/Н.В.Гришина. - 2-е изд., доп. - Москва: Форум: ИНФРА-М, 2019.
12. Груба, И.И. Системы охранной сигнализации. Технические средства обнаружения: справочное пособие / И.И.Груба. - М.: СОЛОН-Пресс, 2013.
13. Душкин, А.В. Аппаратные и программные средства защиты информации: учебное пособие / А.В.Душкин, А.Кольцов, А.Кравченко. - Воронеж: Научная книга, 2017.
14. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019.
15. Направляющие системы электросвязи. В 2-х т. Т. 2. Проектирование, строительство и техническая эксплуатация: учебник для ВУЗов/В.А.Андреев, А.В.Бурдин, Л.Н.Кочановский и др.; под ред. В.А.Андреева. - М.: Горячая линия-Телеком, 2010.
16. Пескин, А.Е. Системы видеонаблюдения. Основы построения, проектирования и эксплуатации / А.Е. Пескин. - Москва: Горячая линия-Телеком, 2013.
17. Портнов, Э. Л. Принципы построения первичных сетей и оптические кабельные линии связи: учебное пособие для вузов / Э.Л.Портнов. - Москва: Горячая линия-Телеком, 2013.

18. Портнов, Э.Л. Электрические кабели связи и их монтаж: учебное пособие/Э.Л.Портнов, А.Л.Зубилевич. - 2-е изд. - Москва: Горячая линия-Телеком, 2010.
19. Программно-аппаратные средства обеспечения информационной безопасности / А.В.Душкин, О.М.Барсуков, Е.В.Кравцов, К.В.Славнов. – Москва: Горячая Линия–Телеком, 2016.
20. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей: учебное пособие для вузов/Е.Б.Алексеев, В.Н.Гордиенко, В.В.Крухмалев и др.; под ред. В.Н.Гордиенко, М.С.Тверецкого. - Москва: Горячая линия-Телеком, 2017.
21. Рябко, Б. Я. Криптографические методы защиты информации: учебное пособие/ Б.Я.Рябко, А.Н.Фионов. – М.: Горячая линия–Телеком, 2017.
22. Скрипник, Д.А. Общие вопросы технической защиты информации/ Д.А.Скрипник. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
23. Субботин, Е. А. Методы и средства измерения параметров оптических телекоммуникационных систем: Учебное пособие для вузов / Е.А. Субботин. - Москва: Горячая линия-Телеком, 2013.
24. Техническая диагностика современных цифровых сетей связи. Основные принципы и технические средства измерений параметров передачи для сетей PDH, SDH, IP, Ethernet и АТМ/И.И. Власов, Э.В.Новиков, М.М.Птичников, Д.В.Сладких; под ред. М.М.Птичникова. - М.: Горячая линия-Телеком, 2017.
25. Чернышев, Е.И. Линейные сооружения связи: учебное пособие для студ. учрежд. СПО/Е.И.Чернышев. - Волгоград: Ин-Фолио, 2010.

Периодические издания:

1. Защита информации Inside.
2. Information Security/Информационная безопасность.
3. Электросвязь.

5 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в ИТКС.	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в ИТКС.	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение
ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в ИТКС с использованием технических средств защиты в соответствии с предъявляемыми требованиями.	- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; - проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение

ПК 3.4. Проводить отдельные работы по физической защите линий связи ИТКС.	выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Экспертное наблюдение
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение Экзамен
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	Экспертное наблюдение Экзамен
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экспертное наблюдение Экзамен
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	Экспертное наблюдение Экзамен

